



Driving towards Success in the Air Force Cyber Mission

Leveraging Our Heritage to Shape Our Future

Lt Gen David S. Fadok, USAF

Dr. Richard A. Raines



Just a few decades ago, we viewed airpower primarily as rated aircrews operating combat aircraft and dropping bombs on targets. Today, it means so much more. For example, 16 of the 18 Airmen whose heroic accomplishments are highlighted in the latest edition of the Air Force chief of staff's *Portraits in Courage* are not flyers, and 15 are enlisted personnel.¹ All of them, however, delivered airpower on the front lines of combat, whether driving convoys, disposing of explosive ordnance, providing security outside the wire, serving as instructors to Afghan and Iraqi forces, or calling in precision strikes from aircraft flying above. In fact, the most recent version of our capstone doctrine document, AFDD 1, *Air Force Basic Doctrine, Organization, and Command*, recognizes this changing nature of

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE OCT 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Driving towards Success in the Air Force Cyber Mission: Leveraging Our Heritage to Shape Our Future				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Research Institute (AFRI) ,155 N. Twining Street,Maxwell AFB,AL,36112				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 8	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



airpower by defining it as “the ability to project military power or influence through the control and exploitation of air, space, and cyberspace to achieve strategic, operational, or tactical objectives.”²

General of the Air Force Henry “Hap” Arnold offered sage counsel when he declared that “we must think in terms of tomorrow.”³ A large part of airpower’s tomorrow will take place in the emerging operational domain of cyberspace. Rapid advancement in computer and communication technologies, as well as the tight coupling of the “digital domain” to physical operations, makes cyberspace increasingly important to military success. The challenges presented by cyberspace reflect its global nature, the political sovereignties it transcends, and the fact that operations take place at the speed of light. By no stretch of the imagination does the United States enjoy the clear, asymmetrical advantage in cyberspace that we do in the land, sea, air, and space domains.

We share information instantly across the World Wide Web by means of e-mail, social networking sites, and other forms of electronic communication. Although this ability has substantially decreased the time necessary to make decisions, it has increased our reliance on communication systems. Information flows through cyberspace at extremely rapid rates, and—unlike traditional kinetic attacks—cyberspace attacks can start, stop, and change completely within a matter of seconds . . . without warning. Consequently, our Airmen must be ready to respond at a moment’s notice—and herein lies the challenge.

The proverbial “laptop and Internet connection” provides entry at extremely low cost into the cyberspace exploitation game. As a result, the modern cyberspace adversary is, and will continue to be, highly agile and innovative. We struggle to produce guidance and policies for cyber operations rapidly and accurately, but adversaries have proven quite adept at developing new, creative methods of cyber exploitation and attack, many times using the restrictions of our own legal system against us. The cyber environment changes so rapidly that one can argue that our policies may be largely outdated when we finally approve them. Furthermore, we face



the real danger that we cannot develop doctrine and tactics rapidly enough to keep pace with changing operational threats in cyberspace.

For years, cyber espionage and exploitation have existed on a global scale. Not limited to nation-states, these actions have also involved actors from industry, organized crime, activist groups, and terrorists. Obviously, motives vary by group, but in most cases, cyber espionage and exploitation are driven by gains in finances and intellectual property. We in the Air Force are concerned about protecting our critical assets and intellectual property as well as prosecuting targets via cyber means as allowed by the *United States Code* and title authorities. To do so, we must create the thought leaders, cyber workforce, operational concepts, and technological capabilities to execute successfully during times of cyber conflict and/or cyber warfare.

Ongoing debates address what constitutes cyber warfare and whether or not we really are at war in cyberspace. This article does not enter into those issues; rather, it suggests how the Air Force and Air University should move forward to lead and support our nation's cyber security needs. Thus, it focuses on analogous lessons learned from history, our position today and what it needs to be, and plans for getting there with respect to our cyberspace capabilities.

Our Heritage: The Air Corps Tactical School

During the years between World War I and World War II, a collection of great minds came together in the Air Corps Tactical School (ACTS), the progenitor of Air University. ACTS brought together some of the brightest people available to define, develop, and demonstrate how best to control and exploit the new domain of airspace. These pioneering aviators used their collective talents to drive the development of technologies needed to implement airpower capabilities. From classroom drawing boards to applied classrooms in the skies, ACTS offered a learning environment for early airpower development and a testing ground for the refinement of proposed concepts and technologies. Students became teachers and vice versa, sharing ideas and concepts for



nearly 20 years. By advancing airpower thought, they exerted a tremendous influence on how we conducted air operations in World War II.

One of these great thinkers, Gen Muir Fairchild, would become the first commander of Air University. When its doors opened in 1946, he determined that this new institution would adopt the motto of ACTS: *Proficimus More Irretenti* (We Make Progress Unhindered by Custom). Since those early days of ACTS, the Air Force has continued to lead the advancement of airpower concepts and capabilities through new, innovative methods for improving our effectiveness in the air domain. In large part, we can attribute these successes to the talented, imaginative men and women aviators who found solutions to problems.

Addressing Today's Cyber Challenges for Tomorrow's Air Force

Much has changed since ACTS established the foundations of airpower. We now find ourselves in a global, instant-access-to-information environment where conflict can begin in the blink of an eye and without apparent evidence. Cyberspace has created a domain in which conflict can go undetected and unattributed. As mentioned above, the cyberspace domain admits players for a low cost of entry, many of them highly educated and skilled. Given the rapidity of cyberspace events, the protection and control of information to assure our mission success are of utmost importance. Exfiltration of information from our cyber assets, as well as attacks on our critical resources, demands that we quickly develop the means to counter these adversarial actions and at the same time develop and mature our capabilities in offensive cyber operations.

The Air Force and Department of Defense (DOD) must have leadership and a workforce capable of understanding how cyberspace can and will be used against us, and how we can utilize it to deliver sovereign options for our national political leaders. We must advance, develop, prove, and deploy those options to our war fighters. Education,



training, research, testing, evaluation, and development must emphasize mission assurance, independent of the operating domain.

Currently, Air Force cyberspace must consider two tasks: creating and sustaining a workforce to meet tomorrow's issues, and developing concepts and capabilities to counter as well as mitigate the efforts of our skilled adversaries. The first task will prove difficult, driven primarily by shrinking defense budgets and commitments to our core mission areas.

Operations in cyberspace will continue to challenge us with unknowns and rapidly emerging threats of ever-increasing complexity. Cyber excellence must be grounded in superior cyber *education and research*. Speed-of-light operations within cyberspace call for rapid, effective development and employment of operational concepts and technological capabilities to help reduce demands on the cyber operator/warrior. Concepts and capabilities must meet the commander's mission needs and ensure effective operations with an extremely high level of certainty.

A Way Ahead: The Cyberspace Air Corps Tactical School

Lately, we have heard several references to the notion that, in terms of cyberspace, we are once again in the interwar years. If true, perhaps it is time to establish a "Cyber" ACTS (C-ACTS), where we can gather critical, strategic thinkers from all the key players in government (both inside and outside Air University) and the private sector for the purpose of advancing thought in our newest domain of cyberspace. A successful C-ACTS would

- Strongly link and leverage talents and resources from education, science, and technology, as well as operational communities.
- House and closely interact with innovators from the above-mentioned communities who possess exceptional credentials in academics, research and development, and experience.
- Provide a forum for creativity, innovation, and exchange, not only to cultivate ideas but also to develop and test prototypes rapidly and to field system(s).



- Strongly couple technological innovations and development with the evolution of tactics and doctrine.
- Blend state-of-the-art education with experiential learning (i.e., “fly” the cyber ideas).
- Closely integrate cyber developments into overall mission-assurance requirements to deliver effective nonkinetic courses of action to the decision maker.

Because we live and operate in a decentralized environment, we should not house a C-ACTS solely within a single organizational structure. We have many cyber-smart organizations that we can and must leverage. At the national level, the Central Intelligence Agency, DOD, Department of Energy, Department of Homeland Security, and Federal Bureau of Investigation possess inherent cyber operations and development capabilities with distinct but sometimes overlapping cyber responsibilities. Within the DOD, US Cyber Command, the National Security Agency, and each of the armed services have cyber organizations chartered to conduct operations under the authority of Titles 10, 18, 32, and 50. DOD service academies can offer foundational cyber education, while institutions such as the Air Force Institute of Technology and the Naval Postgraduate School make available continuing, advanced, and graduate cyber education. The Air Force and Navy boast extensive cyber training capabilities through Air Education and Training Command and Cyber Forces, respectively. The Army and Marine Corps leverage their two sister services' existing education and training capabilities while developing mission-specific capabilities by means of their own Cyber Commands. Furthermore, research and development capabilities reside in the research laboratories of each armed service. Industry and academe also play key roles in the development of both human and technological cyber capital.

Air University is moving ahead with the C-ACTS concept to create a better environment for sharing information and advancing thought. Building upon existing partnerships and developing new ones as appropriate, we seek to work closely with our operational partners in



Twenty-Fourth Air Force and our research and development partners in the Air Force Research Laboratory to ensure the highest return on investment for cyber activities. Across Air University, we have resources supporting C-ACTS. The Center for Cyberspace Research, designated the Air Force Cyberspace Technical Center of Excellence and located within the Air Force Institute of Technology, is charged with coordinating C-ACTS efforts. This tasking complements those issued by the Secretary of the Air Force in 2008 for the Center for Cyberspace Research to “connect the dots” regarding who is doing what in cyberspace education, research, and development.

Final Thoughts

The Air Force is conducting operations during a time of dynamic change. Operations in and through cyberspace will demand new tactics, techniques, and procedures as well as new leadership mind-sets to counter enemy actions. We must rapidly develop and maintain the next generation of cyber leaders and warriors, who will confront a complex information age and the cyberspace domain of operations. We in Air University are up to the challenge of developing and equipping our cyber leaders and warriors with the knowledge and experience they need for mission assurance and operational success. As General Arnold advised, we will continue to think in terms of tomorrow, pursuing progress unhindered by custom in the newest operational domain of cyberspace. ★

Notes

1. Department of the Air Force, *Portraits in Courage: Airmen in the Fight*, vol. 6 (Washington, DC: Department of the Air Force, 2011), <http://www.af.mil/shared/media/document/AFD-110921-035.pdf>.
2. Air Force Doctrine Document 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011, 11, <http://www.e-publishing.af.mil/shared/media/epubs/afdd1.pdf>.
3. H. H. Arnold, *Global Mission* (New York: Harper, 1949), 615.



Lt Gen David S. Fadok, USAF

General Fadok (USFA; MA, Oxford University; MAAS, School of Advanced Airpower Studies, Air University) is commander and president of Air University, Maxwell AFB, Alabama. He provides full-spectrum education, research, and outreach at every level through professional military education, professional continuing education, and the granting of academic degrees. The general leads the intellectual and leadership center of the US Air Force, graduating more than 50,000 resident and 120,000 nonresident officers as well as enlisted and civilian personnel each year. Additionally, he is responsible for officer commissioning through Officer Training School and the Reserve Officer Training Corps. He previously served as commander of the Curtis E. LeMay Center for Doctrine Development and Education and vice-commander of Air University. General Fadok completed graduate studies as a Rhodes Scholar before earning his pilot wings in 1985. A command pilot with more than 4,000 hours, he previously commanded at the squadron, group, and wing levels. He flew combat and combat-support missions in operations Just Cause, Desert Shield, Desert Storm, and Southern Watch. A distinguished graduate of both Squadron Officer School and Air Command and Staff College, as well as a National Defense Fellow, the general received the Secretary of the Air Force Leadership Award in 1988.



Dr. Richard A. Raines

Dr. Raines (BSEE, Florida State University; MS, Air Force Institute of Technology; PhD, Virginia Tech) is director of the Air Force Center for Cyberspace Research, the Department of Defense's Force Transformation Chair, and professor of electrical engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. He serves as a technical consultant to numerous US government organizations and federal cyber security working groups. Dr. Raines has authored more than 150 technical and strategic publications on communications and cyber security. In 2007 he was inducted into the Association of Old Crows' Hall of Fame for his contributions to information operations, and in 2008 he received the Air Force Science and Engineering Educator of the Year award. Dr. Raines is a senior member of the Institute of Electronics and Electrical Engineers.

Let us know what you think! Leave a comment!

Distribution A: Approved for public release; distribution unlimited.

Disclaimer

The views and opinions expressed or implied in the *Journal* are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government.

This article may be reproduced in whole or in part without permission. If it is reproduced, the *Air and Space Power Journal* requests a courtesy line.

<http://www.airpower.au.af.mil>